GROUP A

i. BITC01/0903/2021 GLORIA NJERU
ii. BCSC01/0040/2021 WANYONYI LEVY
iii. BCSC01/0045/2021 ADRIAN APINDI
iv. BITCO1/1519/2021 ERNEST MWAI
v. BITC01/0909/2021 EUCABETH KERUBO

1. Research on the protocols for maintaining confidentiality of email or for secure web transactions
2. Both Windows and Linux differ in file systems and encoding systems. Describe the features of the file systems and encoding systems within each operating system and provide their examples.
3. Discuss four computer security threats and recommend solutions for each
4. OKWS uses database proxies to control what data each service can access, but lab 2 has no database proxies. Explain what controls the data that each service can access in lab 2.
5. The VM-based BackTracker system requires no modifications to the guest OS, but nonetheless makes assumptions about the guest OS. List assumptions that are critical to back-tracking attacks that used high-control events.

GROUP B

i. BCSC01/0014/2021 SETH NGANGA
ii. BITC01/2154/2022 JOSEPH MUNDIA
iii. BCSC01/0035/2021 ALVIN KIPTOO
iv. BITC01/1484/2021 LORENA TERAH
v. BCSC01/1582/2020 TIMOTHY KIPKOECH

1. Research on Malicious logic, and System evaluation and certification.
2. Research on UDP verses TCP traffic in terms of systems security
3. Research on the need of Computer Security
4. In lab 2, logging is implemented by a persistent process that runs under a separate UID and accepts log messages, so that an attacker that compromises other parts of the application would not be able to corrupt the log. Ben Bitdiddle dislikes long-running processes, but still wants to protect the log from attackers. Suggest an alternative

design for Ben that makes sure past log messages cannot be tampered with by an attacker, but does not assume the existence of any long-running user process.

5. Alice finds a suspicious file, /tmp/mybot, left behind by an attacker on her computer. Alice decides to use Backtracker to find the initial entry point of the attacker into her computer. In the following scenarios; would Alice be able to use Backtracker, to find the entry point?
    a. An attacker exploits a buffer overflow in a web server running as root, gets a root shell, and creates the /tmp/mybot file.
    b. An attacker exploits a buffer overflow in a web server running as root, gets a root shell, and modifies the password file to create an account for himself. The attacker then logs in using the new account, and creates the /tmp/mybot file.
    c. An attacker guesses root’s password, logs in, and creates the /tmp/mybot file.

GROUP C

i. BITC01/1486/2020 BONIFACE NGENGOI
ii. BITC01/0925/2021 MARIAM ACHIENG
iii. BITC01/1553/2021 JOSEPH MBUGUA
iv. BCSC01/0007/2021 SOPHIE WANGUI
v. BCSC01/0049/2021 SILA OTIENO

1. Develop a Risk assessment module for Cooperative University
2. Discuss on the types of attacks.
3. Explain back doors and trap doors attacks
4. A company named Vault wants to offer a secure, cloud-based backup system. When the user updates a local file, her Vault client opens a TCP connection to a Vault server, and uses the Diffie-Helman protocol to establish a secret symmetric key *K* with the server. Then, the client generates this string *s*:

s = (documentName, documentContent, userName, userPassword, randomNumber)

and sends the following message to the Vault server:

$$EK(s,\mathrm{HMAC}K(s))$$

where *EK*(*m*) denotes encrypting message *m* using key *K*, and HMAC*K*(*m*) denotes computing an

HMAC message authentication code of message *m* using key *K*. The server decrypts the message, verifies the user's password, and verifies the integrity of the message using the HMAC. If all of the checks succeed, the server stores the document. If the server sees more than 10 messages with the wrong password, all future accesses to that account are blocked. How can a network attacker reliably obtain the user's password?

5. Suppose that a user visits a mashup web page that simultaneously displays a user's favorite email site, ecommerce site, and banking site. Assume that:
    - The email, ecommerce, and banking sites allow themselves to be placed in iframes (e.g., they don't prevent this using X-Frame-Options headers).
    - Each of those three sites is loaded in a separate iframe that is created by the parent mashup frame.
    - Each site (email, ecommerce, banking, and mashup parent) come from a different origin with respect to the same origin policy. Thus, frames cannot directly tamper with each other's state.

    Describe an attack that the mashup frame can launch to steal sensitive user inputs from the email, ecommerce, or banking site.

GROUP D

i. BITC01/1500/2021 LIAN MWAURA

ii. BCSC01/ 0039/2021 ZEPH ASEKA

iii. BCSC01/0019/2021 JOHNSON KANYI

iv. BITC01/0919/2021 JOSEPH KIMANI

v. BOTC01/0905/2021 SHEILA BLESSINGS

1. Research on basic cryptography.
2. Compare symmetric and asymmetric key cryptography
3. Distinguish between the following: Cryptography, Cryptanalysis and Cryptology.
4. Browsing the web through Tor can be slow. This is because user traffic is forwarded between volunteer computers that are scattered across the world, overburdened with traffic, and potentially situated behind slow network connections.

Suppose that CloudCo, a large technology company with datacenters scattered across the world, offers some of its machines to the Tor community for use as entry and exit nodes. CloudCo machines have plentiful RAM and CPU; CloudCo machines also have low latency, high-bandwidth network connections to all major ISPs. By using CloudCo machines as Tor entry and exit nodes, users could ensure that Tor congestion would only exist in the middle of a circuit.

Assume that CloudCo genuinely wants to help Tor users, and that CloudCo configures its machines to faithfully execute the Tor protocol. Why is it still a bad idea for users to employ CloudCo machines as entry and exit nodes?

5. Ben Bitdiddle wants to use Backtracker on his web server running the Zoobar web application. Ben is worried about both SQL injection and cross-site scripting attacks, where an attacker might use the vulnerability to modify the profiles of other users. Ben runs unmodified Backtracker on his server, and uses a known SQL injection vulnerability to test Backtracker, while other users are actively using the site. Ben finds that he cannot effectively track down the attacker's initial entry point, after he detects that one of the user's profiles has been defaced by the attack. Explain why Backtracker is not working well for Ben as-is.

GROUP E

i. BITC01/1522/2021 JIMALDIN HUSSEIN
ii. BCSC01/0003/2021 CYNTHIAJOY MWENDE
iii. BCSC01/0012/2021 EZRA AMANI
iv. BITC01/0889/2021 JAMES GITUIKU
v. BITC01/0908/2021 NEEMA KAIRU

1. Research on the following techniques TACACS +, RADIUS, KERBEROS, VPN, IKE / IPSec.
2. Research on data recovery tools and data recovery procedures
3. Research on any four attacks on Computer System Security
4. Ben Bitdiddle has a smartphone with an always-on voice recognition system, which runs any commands that it hears. Alyssa P. Hacker wants to trick Ben's phone into running a command, but Ben turns off all wireless radios on the phone as a precaution to prevent Alyssa from breaking in over the network, and also keeps his phone in a

locked sound-proof room in hopes of foiling Alyssa. After hearing Kevin Fu's guest lecture, Alyssa figures out how she can get Ben's phone to run a command of her choice, without breaking into Ben's room. What is Alyssa's plan?

5. Explain how an adversary can break into any account on Ben's web site, which uses Ben's modified password scheme described on the previous page. Assume the adversary does not steal the stored passwords from the server.

GROUP F

i. BITC01/0050/2019 MOSES MUICHUHIA
ii. BITC01/0890/2021 IAN MWAI
iii. BCSC01/0041/2021 WAMALWA OSCAR
iv. BCSC01/1534/2021 AQUILA MUTURI
v. BCSC01/0254/2020 EVERLINE WAMBULWA

1. Research on a recent security problem that affected Kenyan systems
2. Research on the importance of biometrics in Computer security.
3. Discuss finger prints registration and verification process.
4. Alyssa wants to learn the identity of a hidden service running on Tor. She plans to set up a malicious Tor OR, set up a rendezvous point on that malicious Tor OR, and send this rendezvous point's address to the introduction point of the hidden service. Then, when the hidden service connects to the malicious rendezvous point, the malicious Tor OR will record where the connection is coming from. Will Alyssa's plan work? Why or why not?
5. Propose a modification of Backtracker that would allow Ben to find the attacker's initial entry point for SQL injection attacks. Be sure to explain how the log, EventLogger, and Graph-Gen would need to be modified for your design, if at all, and whether you need to add any additional logging components. It's fine if your design does not handle buffer overflow attacks, and only handles SQL injection.

GROUP G

i. BITC01/0894/2021 ISAAC MAINA
ii. BITC01/0891/2021 WAMBUI LUCY
iii. BITC01/0901/2021. ERICK MOTI
iv. BCSC01/0042/2021 MICHAEL MOUNDE

v. BCSC01/0034/2021 GEORGE JESSE

1. Research on one-time pass-words, token cards / soft tokens
2. Research on transposition technique.
3. Convert plain text to Cipher text using Rail Fence technique “COMPUTER ENGINEERING”.
4. Ben’s modified Backtracker system still cannot catch the attacker’s initial entry point for the Zoobar profile worm, which spreads through a cross-site scripting vulnerability. Propose a modified design for Backtracker that can track down the source of a XSS attack like the profile worm.
5. Bob is running a hidden service on top of Tor, and wants to know how frequently he should choose new introduction points. Bob cares about his identity not being exposed, and about the availability of his service. Help Bob make an informed choice by explaining the costs and benefits of rotating introduction points either more or less frequently.

GROUP H

i. BITC01/0893/2021 PURITY NJERI

ii. BITC01/0663/2021 SIMON MUMO

iii. BCSC01/0006/2021 COLLINS KAMAU

iv. BCSC01/0005/2021CHARLES MAINA

v. BITC01/0898/2021 PERIS ANN

1. Research Kenyan laws regarding computer security,
2. Research on the concept of Kerberos
3. Research on the different password selection criteria
4. Suppose that an adversary steals a laptop protected with BitLocker in TPM mode, and wants to gain access to the data on the BitLocker-encrypted partition. The adversary discovers a buffer overflow in the BIOS code that can be exploited to execute arbitrary code by a specially-crafted USB drive plugged in during boot. How can the adversary gain access to the encrypted data? Be as specific as possible: what operations should the adversary’s injected code perform, both on the main CPU and on the TPM?

5. Bob is running the privilege-separated Zoobar web site on a KeyNIX system, using code from lab 3. Suggest a way in which Bob can modify the Zoobar server-side code to take advantage of KeyKOS capabilities to improve the security of his site, in a way that he wouldn't be able to do on Linux.

GROUP I

i. BITC01/0913/2021 AURA MAURAH
ii. BITC01/0892/2021 MARY WAMBUI
iii. BITC01/2155/2022 EMMANUEL MUTAI
iv. BCSC01/0048/2021 AUSTINE OCHIENG
v. BCSC01/0010/2021 PETER WAGUCHU WAINAINA

1. Research on the various security services and procedures.
2. Research on the types of firewall.
3. Discuss packet filter with diagrams.
4. Bob is developing a new web site, and wants to avoid the problems described in the ForceHTTPS paper. He uses HTTPS for all of his pages and marks all of his cookies "Secure". Assuming Bob made no mistakes, is there any reason for Bob's users to install the ForceHTTPS plugin and enable it for Bob's site? Explain why or why not.
5. Alice wants to read Bob's email, and intercepts all network packets ever sent and received by Bob's workstation (which is the only computer that Bob uses). However, Alice does not know Bob's password to access Bob's post office server, and Bob's packets to and from the post office server are protected by Kerberos.
   a. Suppose that after Bob reads and deletes all of his mail, Alice learns what Bob's password was. Describe how Alice can obtain Bob's past messages.
   b. To prevent Alice from reading any more messages, Bob ensures that Alice cannot intercept any subsequent network traffic, and changes his Kerberos password. Could Alice still read Bob's mail after this? Explain why not or explain how.

GROUP J

i. BITC01/2407/2022 SHADRACK MACHARIA
ii. BITC01/0915/2021 EUGENE KIRIAGO
iii. BCSC01/0010/2019 ELIJAH OUMA

iv. BCSC01/0032/2021 DAISY CHEBET

v. BITC01/2156/2022 FAITH WANJIRU

1. Develop a Security policy for Cooperative University
2. Research on host based IDS with its advantages and disadvantages
3. Research on the steps for hardening applications
4. Ben Bitdiddle wants to secure his SSL server against RSA timing attacks, but does not want to use RSA blinding because of its overhead. Instead, Ben considers the following two schemes. For each of the schemes, determine whether the scheme protects Ben's server against timing attacks, and explain your reasoning.
   a. Ben proposes to batch multiple RSA decryptions, from different connections, and have his server respond only after all the decryptions are done.
   b. Ben proposes to have the server thread sleep for a (bounded) random amount of time after a decryption, before sending the response. Other server threads could perform computation while this thread is asleep.
5. Bob logs into an Athena workstation, which uses Kerberos to obtain a ticket for bob@ATHENA.MIT.EDU, and then runs Bob's mail client, which contacts Bob's post office server to fetch new messages.

   Alice doesn't want Bob to know about an upcoming event, which was announced to Bob via email. To this end, Alice plans to intercept Bob's communication with his post office server, and to pretend that Bob has no new mail. Alice can observe and modify all network packets sent by Bob. How does Kerberos prevent Alice from impersonating Bob's mail server? Be as specific as possible; explain how Bob can tell between Alice and the real mail server in terms of network packets.

GROUP K

i. BITC01/0892/2021 MARY WAMBUI

ii. BITC01/0900/2021 GABRIEL MWASHIGHADI

iii. BITC01/0916/2021 ALLAN JAMLECK NDUNGU

iv. BCSC01/1551/2021 DANIEL WEGA

v. BITC01/2157/2022 NICKSON KIPRUTO

1. Research on Protecting DNS, NIS, Proxy, e-mail, WWW, FTP, NFS. Firewalls, NAT.
2. Explain simple columnar transposition technique with algorithm and example

3. Research on software piracy and the types.
4. An "Occupy Northbridge" protestor has set up a Twitter account to broadcast messages under an assumed name. In order to remain anonymous, he decides to use Tor to log into the account. He installs Tor on his computer (from a trusted source) and enables it, launches Firefox, types in www.twitter.com into his browser, and proceeds to log in.

   What adversaries may be able to now compromise the protestor in some way as a result of him using Tor? Ignore security bugs in the Tor client itself.
5. The protestor now uses the same Firefox browser to connect to another web site that hosts a discussion forum, also via Tor (but only after building a fresh Tor circuit). His goal is to ensure that Twitter and the forum cannot collude to determine that the same person accessed Twitter and the forum. To avoid third-party tracking, he deletes all cookies, HTML5 client-side storage, history, etc. from his browser between visits to different sites. How could an adversary correlate his original visit to Twitter and his visit to the forum, assuming no software bugs, and a large volume of other traffic to both sites?

GROUP L

i. BITC01/2043/2020 MAINGI SAMUEL
ii. BCSC01/0020/2021 LAWRENCE FADHILI
iii. BITC01/2070/2022. NDIRANGU M NINIET NYAWIRA
iv. BCSC01/0037/2021 BETH ANJELA OWALA
v. BITC01/2071/2022 WANJIRU TEKLA MUMBI

1. Research on Cryptographic protocols.
2. Research on individual user responsibilities in Computer Security
3. Research on the need for firewall and explain one of the type of firewall with a diagram
4. Suppose a malicious XFI module wants to circumvent XFI's inline checks in its code. To do so, the module allocates a large chunk of memory, copies its own executable code to it (assume XFI is running with only write-protection enabled, for performance reasons, so the module is allowed to read its own code), and replaces all XFI check instructions in the copied code with NOP instructions. The malicious module then

calls a function pointer, whose value is the start of the copied version of the function that the module would ordinarily invoke. Does XFI prevent an attacker from bypassing XFI's checks in this manner, and if so, what precise instruction would fail?

5. Alice is using the VM-based BackTracker to analyze a compromised server, where an attacker obtained some user's password, logged in via SSH, exploited a buffer overflow in a setuidroot program to gain root access, and trojaned the login binary, all using high-control events that are still stored in the event logger. How can Alice figure out what *specific* vulnerability in the setuid-root program the attacker exploited? In what situations would this be possible or not possible?

GROUP M

i. BITC01//1512/2021 MEGAN MWAURA

ii. BCSC01/0050/2021 ANTHON NYAMERA

iii. BITC01/0926/2021 CINDI MARION

iv. BCSC01/0038/2021 BILHA ACHOLA

v. BCSC01/0015/2021 KELVIN MUTUGI

1. Research on protecting the network and operating system services.
2. Research on e-mail security techniques (protocols).
3. Research on intrusion detection system.
4. Suppose a program has a buffer overflow vulnerability which allows an attacker to overwrite a function pointer on the stack (which is invoked shortly after the buffer is overflowed). Explain what attacks, if any, an attacker would be able to mount if the same program is run under XFI. Be specific.
5. Alice works for a bank that wants to implement an electronic currency system. The goal of the electronic currency system is to allow users to exchange *coins*. There is exactly one type of coin, worth one unit of currency. Alice's bank maintains one server that initially hands out coins. The system should allow user *A* to give user *B* a coin even if the two users are disconnected from the rest of the world (i.e., cannot talk to the bank or to any previous holders of that coin). Furthermore, it should be possible for user *B* to now give a coin to user *C* without having to contact anyone else. It should be impossible for user *A* to "double-spend", that is, to give the same coin to two different users.

Design an electronic currency system assuming each user has a TrInc trinket. Assume each trinket's public key is signed by the bank, that everyone knows the bank's public key, and that all trinkets are tamper-proof and trustworthy.

Explain three aspects of your design:

a. What is the representation of a coin that a user has to store? (It's OK if this representation is not constant size.)
b. How does user *A* send a coin to user *B*?
c. What should user *B* do to verify that it has received a legitimate coin?

GROUP N

BCSC01/0009/2021 GRACE KABERA
BCSC01/0043/2021 RUTH KENYANYA
BITC01/0932/2021 KEITH MAZENGE
BITC01/2406/2022 DAVID MUIRURI
BITC01/0914/2021 DAVIES ONGORO
BITC01/0917/2021 JABEZ MAKUBO

1. Research on potential network security threats.
2. Research on host based IDS.
3. Research on TLS and its layers
4. Suppose a program has a traditional buffer overflow vulnerability where the attacker can overwrite the return address on the stack. Explain what attacks, if any, an attacker would be able to mount if the same program is run under XFI. Be specific.
5. Alice's bank gives up on the trinket idea as being too costly. Instead, Alice is now designing a banking application for Android. She is worried that users of her banking application may be tricked into entering their bank account information into another look-alike application, because there's no reliable way for a user to tell what application he or she may be interacting with.

   For example, there's no way for a user to look at the screen and tell what application is currently running. Even if a user initially runs on a legitimate banking application, a malicious application can start an activity right after that, and display an identical screen to the user. Finally, applications can use full-screen mode to completely replace the entire Android UI.

Propose a design in which users can safely enter their credentials into a banking application. Your proposed design can involve changes to the Android system itself. Unmodified existing Android applications *must* continue to work in your new design (though if you change the UI as part of your design, it’s OK if the applications look slightly different as a result). It’s fine to require sensitive applications (e.g., Alice’s new banking application) to do things differently in your design.